FACTSHEET

Open Finance should not mean an open bar for consumer data

Open Finance is a market mechanism that gives third-party financial service companies, such as payment subsidiaries of big tech giants access to consumers' financial data. It gives third parties access to the data that banks – and in future potentially other financial institutions - hold about consumers. The aim is to promote innovative new financial apps and services, which these companies offer, and for which access to these data is necessary.

In exchange, banks and other financial institutions now want access to all types of data that third parties – like big techs - hold about consumers. This request for data is called '**reciprocity**'. Some banks are now referring to this as creating a 'level playing field'. This fact sheet explains why consumer organisations are opposed to reciprocity.

Background

The 2007 Payment Services Directive (PSD1) allowed non-banks - called 'payment institutions' to provide payment services to consumers. But it quickly became clear that these third-party payment institutions would not be able to work without access to consumers' payment accounts. This is because banks have a monopoly on deposits, such as the payment of salaries. Accordingly, the 2015 update to the Directive (PSD2) gave payment institutions the right to access consumers' payment accounts with their consent – and obliged banks to set up systems to make this access possible.

Two kinds of payment institutions have emerged so far: 1) Payment Initiation Services (PISP), which make payments on behalf of consumers and; 2) Account Information Service (AIS), which provide various kinds of financial services (account aggregation and management, credit, insurance).

These so-called 'non-banks' now want to offer other services, beyond PISP and AIS. But for this they need access to more data, which banks currently hold. This obligation for banks to provide access for third parties to consumers' financial data, including payment account and other data, is justified by a market failure. As banks have privileged information about their clients' financial information, non-bank service providers cannot, for example, develop apps to show consumers whether they have the best credit or insurance provider. This makes competition impossible as non-banks cannot access the information needed to provide these financial services.

BEUC agrees with the idea of Open Finance on the condition that the existing rules about consumer consent and the protection of consumers' financial data are improved. See our paper, 'Consumer-friendly Open Banking' for more information.

What is reciprocity?

In recent years, several big tech companies have set up payment subsidiaries (eg. Apple Pay or Google Pay). They are classed as payment institutions or 'eMoney' institutions according to PSD2. This gives them the ability to access the consumer data that banks hold.

The banking industry now argues that if third parties – such as big tech payment subsidiaries - can access the data they hold on consumers, banks – and potentially other financial institutions in the future - should get access to all types of consumer data the third parties hold (ie. 'reciprocity').

Lucy visits her bank to take out insurance for her new car. Little does she know, her bank is helping itself to all of the data that Big Tech holds about her. This is called 'reciprocity' – in return for third parties' access to Lucy's financial data, banks and other financial institutions are calling for reciprocal data access to consumers personal online data, such as Lucy's online search or social media data. Open Finance shouldn't mean an open bar for data!

Why reciprocity is unacceptable?

1. **RISKS FOR CONSUMERS' CONTROL OVER THEIR PERSONAL DATA.** Consumers might have a fair idea about what their bank knows about them, but much less so when it comes to third parties like big techs. These companies know much more about consumers than banks, often collecting and combining data related to all aspects of a consumers' life. Through geo-location, for example, about the places a person has visited; their sporting or leisure habits; data about friendship networks, chat history, opinions and beliefs or even online search and browsing history. Consumers are often not aware of how much data these companies have about them (which is already problematic on its own). Reciprocity means consumers would be asked to give their banks access to all kinds of personal data, perhaps unaware about what they are giving access to. It is also unclear how such personal information could help banks and other financial institutions improve their services and why it would be necessary to grant such access. At a time when consumers need more control over their personal data, reciprocity would mean greater risks and less control from a consumer data protection perspective.
2. **CONSUMER CONSENT NEEDS TO BE REINFORCED.** Existing means to obtain valid consumer consent are insufficient. Users tick a cookie box to access a website, for example, without any idea of the consequences of this agreement. When granting banks access to personal data held by other companies, consumers would find themselves in a similar situation. For a start, their consent cannot be considered meaningful and informed when they are not aware of which data they would be giving access to and of the consequences. Consumers might also be 'forced' to give blanket access to all their data held by a company, without any choice or sufficient transparency as to the purpose. This is not an issue exclusive to reciprocity, but it becomes even more problematic given the sensitivity of the financial services area. That is why it is necessary to review the conditions in which consumers can validly consent to enable access to this data.
3. **NO MARKET FAILURE.** Reciprocity makes sense for financial data (or non-financial data necessary to provide a financial service). But it cannot extend to non-financial data that are not necessary to provide a financial service. Banks' request to extend reciprocity to these types of data (e.g. your shopping habits, your friends, your movements) is not justified by any market failure. This is because banks can still provide the service without such extensive consumer profiling.

Open Finance and GDPR

The use of personal data in the EU is regulated by the General Data Protection Regulation (GDPR). When accessing financial data, payment institutions could have access to a wide range of information about the consumer, some of which is potentially sensitive.

The GDPR applies to Open Finance, meaning amongst other things that:

- Data must be processed in a lawful, fair and transparent manner;
- The quantity of personal data collected must be strictly limited to what is necessary for a speci-
- fic purpose;
- Data should be used for a specific purpose only and not for other incompatible purposes;
- Explicit consent should be required for profiling based on financial data.

SURVEILLANCE SOCIETY?

A myriad of digital players has been and continues to closely follow consumers' every move, both online and offline. Surveillance has become the dominant business model of the internet and might soon be the reality in all business sectors. Consumers' freedom, rights, autonomy and self-determination are all at risk. Every action is monitored, and a huge amount of personal data is being collected and scrutinised for commercial purposes. This is problematic from a data protection and privacy perspective, but consumers' behaviour and decisions are increasingly influenced in ways beyond their knowledge, understanding and control. It would be very dubious if, through reciprocity, financial institutions – just like the tech giants – were to also amass data about all aspects of our daily lives. Open Finance should offer consumers innovative new financial services, not open the door for them to be profiled and manipulated.